REMARKS

Several changes to the specification have been made voluntarily to correct typographical errors.

TERMS AND USAGE DEFINITIONS

The following terms used herein are intended to be interpreted with the following definitions.

1. Firewall: As used herein, the firewall also provides for Virtual Private Network encryption in addition to providing firewall services. It can be done in hardware or software. Numerous prior art devices exist that implement firewall, VPN or both. In our usage, Firewall represents either hardware or software or a combination of both that both provides firewall security and VPN services to encrypt AlterWAN packets for transmission over the internet on a private tunnel which also happens to be the high bandwidth, low hop count, low latency AlterWAN data path described below.

2. CSU (Channel Service Unit): This is a typical term used for the device that connect the LAN to the WAN in T1 prior art networks. Our use of the term CSU is intended to be generic and to refer to any adapter to take digital packets and put them in a proper form for transmission on whatever data or signal path is used to connect the source and destination sites to the participating ISX/ISP sites which provide the high bandwith, low hop count, low latency AlterWAN data path

3. ISX/ISP: numerous terms exist to identity internet service providers. These two terms have been chosen to mean an internet service provider who can route data packets onto data paths on the internet. The term "participating ISX/ISP" means the specially selected ISX/ISPs selected in the manner described below and whose routers have been configured to route AlterWAN data packets onto the high bandwidth, low hop count, low latency AlterWAN data path.

4. Route Statement: any statement used in a device that controls the path of data packets on the internet.

ANTICIPATION REJECTION

Claims 1-6 have been rejected as anticipated by Provino, US 6,557,037. The Examiner is repectfully requested to withdraw this rejection as incorrect.

The claimed invention is about route control to force routing through the internet to be along high bandwidth, low latency, low hop count data paths. Confidentiality is provided, but this is a sideshow. The invention is about solving the problems that have plagued applications that have attempted to use the internet as a WAN backbone to commercial failure: lack of quality of service which leads to latency and loss of data. Solving this problem is all about route control to force AlterWAN™ network (hereafter just Alterwan) packets to be routed along high bandwidth,

low latency, low hop count paths so there is little latency and little lost data because of congestion.

Route control in the claimed invention involves putting one of the IP addresses that is predetermined to be one of the IP addresses in the Alterwan nework in the destination address field of the Alterwan ip packets. the routing statements in the routing tables at the source site and the routing statements in the routing tables in the intermediate ISX/SIP sites are modified to include recognition of packets with one of these special, predetermined Alterwan IP addresses. When such a packet arrives at the edge source router 18 at the source site, it knows that it is an Alterwan packet and it needs to be put on the dedicated local loop data path 22 to the first participating ISX 24. When the packet arrives at the first participating ISX 24, the routing tables there recognize the packet as an Alterwan packet and route the packet onto a high bandwidth, low latency, low hop count data path 50 which has been previously tested and is guaranteed not to be oversubscribed and to have sufficient bandwidth and traffic volumes so as to provide low latency and high quality of service. This same process happens at ISP 48 and ISP 54 and destination router 42. That is, the IP address in the destination address field is recognized as an Alterwan address and forces the routing of the packet to be along a predetermined data path that provides high bandwidth and low latency. That is how the Alterwan network solves the problems with prior technologies such as voice-over-IP which have been commercial failures in attempting to use the internet as a backbone.

Support for this argument is found in the Summary of the Invention in the specification starting at page 6, line 11, to wit:

> Only packets identified at the source end firewall with a destination IP address at the other end of an AlterWAN "private tunnel" have the payload of the packet encrypted before being sent. Once they are encrypted, they are sent across the preplanned route to the destination where the far end firewall recognizes the IP address of the packet as being addressed to it. Only those packets are decrypted and transmitted to the device to which they are addressed and other packets that are not AlterWAN packets are either rejected or routed to some other device which is not part of the AlterWAN network.
>
> In other words, the quality of service problem that has plagued prior attempts is solved by providing non-blocking bandwidth (bandwidth that will always be available and will always be sufficient) and predefining routes for the "private tunnel" paths between points on the internet between ISX facilities. Participating ISX facilities agree to provide non-blocking bandwidth between their sites.

And at page 7, line 27, we teach:

In other words, the quality of service problem that has plagued prior attempts is solved by providing non-blocking bandwidth (bandwidth that will always be available and will always be sufficient) and predefining routes for the "private tunnel" paths between points on the internet between ISX facilities. Participating ISX facilities agree to provide non-blocking bandwidth between their sites.

And at page 8, lline 4, we teach:

Browsers at workstations at customer AlterWAN sites however can be pointed to any website on the internet and can send and receive packets to and from those sites without restriction. Those packets are referred to herein as conventional packets, and they get to their destinations by conventional internet routing and do not pass through the private tunnels created by the AlterWAN data structures.

The AlterWAN data structures really are just IP addresses and associated data in the firewalls and routers along the tunnel that cause the packets to travel the low hop count path. The AlterWAN data structures will vary from customer to customer depending upon which sites are to be linked and the locations and IP addresses of the participating ISX/ISP providers through which the hops of the private tunnel will pass.

At page 8, line 14 we teach:

Finally, all species in the genus of the invention will solve the bandwidth bottleneck that has plagued prior attempts to use the internet as a WAN backbone. This is done by implementing AlterWAN™ routing strategies. An AlterWAN data path extends from a source router (having a channel service unit to interface between the packet world of routers to the physical and media access control and/or signalling protocols of the telephone line) through a sufficiently high bandwidth dedicated local loop line to the first participating ISX or Internet Service Provider (ISP) that is a participating provider of AlterWAN™ network services. From there it extends along a data path between other participating ISX providers along a data path which is guaranteed to have sufficient bandwidth to be able to handle the worst case bandwidth consumption of the customer. In the claims, such an ISX or ISP provider is referred to as a "participating ISX/ISP". All the ISX or ISP facilities that are participating in the AlterWAN™ network structure have fiber optic or other high bandwidth data paths such as OC3 or OC12 data paths available to them to send data to other ISX/ISP facilities that are participating in the AlterWAN™ network. It is these high bandwidth links which are referred to as "core bandwidth" between participating ISX/ISP facilities. It is this core bandwidth over which AlterWAN™

"private tunnel" traffic is routed on the internet backbone.

The critical part of the invention (getting the right IP addresses in the destination address field) is taught at page 11, line 26:

> **More specifically, at each end of a private tunnel, a packet addressed to any of the IP addresses of devices at the other end of a private tunnel are recognized as packets that need to be converted to AlterWAN packets, encrypted by the firewall and encapsulated in another IP packet having as its destination address the IP address of the untrusted side of the firewall at the other end of the private tunnel. The composite AlterWAN packet is comprised of the encrypted original IP packet with an AlterWAN packet header which has as its destination address the IP address of the untrusted side of the destination firewall. At the firewall at the other end, these incoming AlterWAN packets will recognized because their destination addresses match the IP address of the untrusted side of the firewall.** The firewall then strips off the AlterWAN packet header of the encapsulating packet and decrypts the original IP packet that was encapsulated using the same encryption algorithm and key or keys that were used to encrypt it. The decrypted packet then has an IP packet header which has a destination address which matches the IP address of some device on the LAN on the trusted side of the destination firewall. The decrypted packet is then put on the destination LAN and makes its way to the device to which it was addressed.

(emphasis added)

And at page 30, line 4 we teach what happens to conventional packets which do not have as their destination address the IP address of a device at the other end of the Alterwan data path:

> Any conventional IP packets are also routed into dedicated data path 22, **but these conventional data packets are not part of the AlterWAN private tunnel because their destination addresses are not the address of the destination at the other end of the tunnel.**

(emphasis added)

So the bottom line is that it is the destination IP address in the Alterwan packets that is where the rubber meets the road. It is this IP address which is recognized by the routers of the ISX and ISP partners and which causes AlterWAN packets having this IP address to be routed into a high bandwidth, low latency data path to the next participating ISX where the same thing happens. This continues to happen so Alterwan packets go only to participating ISX locations and at each of those locations, the routing tables have been modified to recognize the IP address in Alterwan

packets as requiring that they be routed along the pre-arranged, pre-tested high bandwidth, low latency, low hop count data path. **It is the putting of specified IP addresses in the destination address field and programming the source and destination routers and the routers of the participating ISX/SIP's to recognize these IP addresses and route these Alterwan packets differently than other packets which solves the quality of service problem.**

Provino is not addressed to this same quality of service problem. In his background section, Provino notes three problems: 1) the need for name servers (col. 1, line 36 to col. 2, ine 11); 2) the need for confidentiality when using the internet as a backbone (col. 2, lines 11-36); 3) control of access of a company's private LAN to intruders from the internet using firewalls and gateways and the fact that the name servers outside do not know the names of the devices inside on the private network (col. 2. lines 37 - 56).

None of these problems Provino addresses involves controlling routing out on the internet to steer AlterWAN packets into high bandwidth, low latency, low hop count data paths. As a result, Provino does not teach the critical element of the invention: recognition of specific IP addresses in Alterwan packets and routing those Alterwan packets differently than other packets so that they travel in a high bandwidth, low latency, low hop count data path. This data path has been pretested to make sure it will handle the bandwidth and speed requirements of a customer application.

That Provino does not teach the same invention is evidenced by the following passages from his specification. In the passage, the Examiner cites, starting at Col. 9, line 32:

> Communications between devices external to the virtual private network 15, such as device 12(m), and a device, such as a server 31(s), inside the virtual private network 15, may be maintained over a secure tunnel between the firewall 30 and the external device as described above to maintain the information transferred therebetween secret while being transferred over the Internet 14 and through the ISP 11. A secure tunnel between device 12(m) and virtual private network 15 is represented in FIG. 1 by logical connections identified by reference numerals 40, 42, and 44; it will be appreciated that the logical connection 42 comprises one of the logical connections 41 between ISP 11 and Internet 14, and logical connection 44 comprises one of the logical connections 43 between the Internet 14 and the firewall 30.
>
> Establishment of a secure tunnel can be initiated by device 12(m) external to the virtual private network 15. In that operation, the device 12(m), in response to a request from its operator, generates a message packet for transfer through the ISP 11 and Internet 14 to the firewall 30 requesting establishment of a secure tunnel between the device 12(m) and firewall 30. **The message packet may be directed to a predetermined**

> **integer Internet address associated with the firewall 30 which is reserved for secure tunnel establishment requests, and which is known to and provided to the device 12(m) by the nameserver 17. If the device 12(m) is authorized to access a server 31(s) in the virtual private network 15, the client 12(m) and firewall 30 engage in a dialog, comprising one or more message packets transferred therebetween over the Internet 14.** During the dialog, the firewall 30 may provide the device 12(m) with the identification of a decryption algorithm and associated decryption key which the device 12(m) is to use in decrypting the encrypted portions of message packets which the virtual private network transmits to the device 12(m).

Note that there is no mention anywhere in this passage of recognition of the IP address of firewall 30 and that recognition causing the packets addressed to the IP address of firewall 30 to be routed into a pre-tested, high bandwidth, low latency data path which an ISX has agreed to provide for all packets having the IP address of firewall 30. This is the essence of the invention and it is how the quality of service problem of attempting to use the internet as a WAN backbone is solved. Provino therefore does not teach the same invention as is claimed.

Other passages buttress the conclusion that Provino does not teach recognitions of special IP addresses and routing through high bandwidth, low latency data paths. For example, at col. 6, lines 56-59 Provino teaches:

> The device 12(m) transfers the request message packet(s) to the ISP 11. The ISP 11, in turn, will transfer the message packet over the Internet to the device 13.

No mention of special routing of the request into a high bandwidth, low latency data path is made. Similar passages occur at Col. 7, lines 2-9:

> ... if the requested service is to initiate the transfer of information from the device 13 as a storage server to the device 12(m) as client, the device 13 will generate one or more response message packets including the requested information, and transmit the packet(s) over the Internet14 to the ISP 11. The ISP, 11, in turn, will transfer the message packet(s) to the device 12(m). On the other hand, if the requested service is to initiate processing by the device 13 as a compute server, the device 13 will perform the requested computation service(s). In addition, if the device 13 is to return processed data generated during the computations to the device 12(m) as client, the device 13 will generate one or more response message packet(s) including the processed data and transmit the packet(s) over the Internet 14 to the ISP 11. The ISP 11, in turn, will transfer the message packet(s) to the device 12(m). Corresponding operations may be performed

> by the devices 12(m) and 13, ISP 11 and Internet 14 in connection with other types of services which may be provided by the server devices 13.

Again, no mention of special routing of the request into a high bandwidth, low latency data path is made anywhere in this passage. There is no mention of special recognition of specific IP addresses and no mention high bandwidth, low latency data paths into which specific packets recognized to have specific IP addresses are routed.

A similar passage occurs at Col. 8, lines 54-57:

> After the packet generator 22 receives the integer Internet address, it can generate the necessary message packets for transmission to the device 13 through the network interface 21 and ISP 11.

All these passages indicate just normal routing occurs and that does not solve the Quality of Service problem. **The invention is not a Virtual Private Network, although VPN technology is incorporated only to supply the necessary privacy.**

The way the invention differs over a VPN is that in a VPN, although the VPN packets have as the destination address the IP address of the firewall at the other end of the tunnel, this IP address causes no special routing in the intermediary ISX/ISP routers. In VPN, those routers have not be configured to recognize packets with that IP addresses and route those packets into a high bandwidth, low latency, low hop count data path.

The invention is not a conventional VPN. A VPN piggybacks on top of the invention, and it is very easy to get the invention and a VPN confused. Hopefully, the above explanation will clarify matters.

EXPLANATION OF THE AMENDMENTS TO THE CLAIMS AND SPECIFICATION OF THE CLAIM LIMITATIONS THAT DISTINGUISH THE INVENTION OVER PROVINO, US 6,557,037

Claim 6: The preamble was amended to move a phrase for better structure. The first element was amended voluntarily to remove local loop because that phrase could be interpreted to limit the first leg to a telco line when it could be anything such as cable modem and HFC, wireless, etc.

The source router element was amended to: 1) point out how the routing tables of the source router have been configured to recognize AlterWAN packets by the destination IP addresses; 2) specify that these predetermined destination IP addresses are specific IP addresses which have been assigned to an AlterWAN private tunnel3) to define what an AlterWAN packet is; 4) to define what an AlterWAN private tunnel is in terms of it being a data path which is always high bandwidth, low latency between predetermined ISX/ISP providers, the path having been pretested to ensure it has adequate bandwidth and low latency and that

AlterWAN packets always get routed into it.

The claim element regarding the routers at the participating ISPs has been amended as follows (the limitations in bold distinguish the claimed invention over Provino):

> one or more internet data paths coupled to routers of said predetermined ~~other participating~~ ISX/ISP providers of internet services, **said routers having their routing tables configured to recognize said AlterWAN packets by their destination addresses and to cause said routers to route AlterWAN packets into said AlterWAN private tunnel data path**, each ~~besides said source ISX/ISP provider including a router at an endpoint participating ISX/ISP provider, said routers of said source and endpoint ISX/ISP providers and said other participating ISX/ISP providers functioning to implement a predetermined private tunnel data path for said AlterWAN packets coupling a router of said source ISX/ISP provider to a router of said endpoint participating ISX/ISP provider through said routers of said other participating ISX/ISP providers, said source and endpoint ISX/ISP providers and~~ said predetermined ~~other~~ ISX/ISP ~~providers being providers~~ provider being a provider of internet services who has ~~have~~ contracted to provide routing of AlterWAN packets into said AlterWAN private tunnel data path, **said AlterWAN private tunnel data path being at least one of said internet data paths which has ~~and who have~~ been pretested to verify that said data path does ~~they do~~ in fact provides a low hop count data path having ~~portion of a data path between a said source site and a said destination site for said AlterWAN packets with~~ an average available bandwidth along each ~~said~~ portion of said data path travelled by said AlterWAN packets which ~~each ISX/ISP provider provides which substantially~~ exceeds the worst case bandwidth consumption of AlterWAN packet traffic between said source site and said destination site;**

This amendment is supported by the following passage in the specification from page 15, line 9:

> **AlterWAN packets get routed at the first ISX/ISP 24 into a high bandwidth data path 50 to the next participating ISX/ISP 48 in the AlterWAN network. Data path 50 is selected for the AlterWAN packets by the preselected ISX/ISP and peer level predefined routing between participating ISX/ISP's.** This allows AlterWAN traffic to be transported between locations utilizing the naturally existing routes but those routes are selected so as to be high bandwidth and low hop count. Each router in the participating ISX/ISP facilities connects and communicates in the same fashion. AlterWAN networks, by design, require selection of the ISX/ISP partners for any given network based on many factors including the ease of implementation by utilizing naturally occurring or other existing high bandwidth, low hop count routes. AlterWAN designers pre-test these routes

by performing a minimum of a ping test and traceroute test to verify the path data that AlterWAN packets will take through the private tunnel that is to be implemented as an AlterWAN connection. **AlterWAN partners do not normally need to add special routes, but implementing AlterWAN network designs that follow existing known paths does not preclude the addition of special routing from time to time as needed to afford better routing. By such a process, an AlterWAN network does not require each participating ISX/ISP to make alterations to their equipment for each "private tunnel" created but rather transparently utilizes the high bandwidth peer level connections between ISX/ISP's. However, the invention does not preclude use of ISX/ISP providers who have altered their routing tables so as to insure that AlterWAN packets get routed along high bandwidth, low hop-count data paths while non-AlterWAN packets get routed along other data paths.** Participating ISX/ISP's are selected in part based on their ability to use these natural routes to form low hop count connections between the ends of an AlterWAN private tunnel or by entering into a special deal with one or more other participating ISX/ISP's to implement special peering arrangements and/or routing between each other to allow only AlterWAN traffic to use these special low hop count high bandwidth connections forcing non AlterWAN traffic to follow other natural routing that does not provide the bandwidth and or hop counts that meet the AlterWAN requirement.

(emphasis mine)

What the bold passages highlighted in this quote mean is this: <u>the AlterWAN packets are recognized by the participating ISX/ISP routers and are routed into the predefined high bandwidth, low latency, low hop count data path; this is done using existing route statements in the ISX routers if they exist or by adding the statements if necessary to make sure this happens.</u>

This distinguishes from the Provino reference where no special routing is forced at the ISPs and they route the VPN packets just like any other packets. Although in VPN a special IP address may be added to a VPN packet as the destination address (the IP address of the terminating firewall at the other end of the tunnel), *this IP address does not get specially recognized in the ISPs and cause a special routing into a high bandwidth, low latency path in the prior art Provino reference.* That is the basic difference between the invention and VPN technology like Provino.

Claim 7 distinguishes over Provino by the underline major addition to the following claim element:

at said source firewall, comparing the destination address in each said received IP packet to an IP address of a computer at said destination site of said customer, and if an IP

packet has as its destination address the IP address of a computer or other computing device at said destination site (hereafter referred to as an AlterWAN inner packet), concluding said IP packet is an AlterWAN inner packet ~~payload~~ which needs to be transmitted ~~via a virtual private network over the internet~~ to said computer or other computing device at said destination site via a high bandwidth, low latency, low hop count data path using said internet as a backbone and connecting said source site to said destination site and having an average available bandwidth which exceeds the worst case bandwidth consumption of packets traveling between said source site and said destination site (hereafter referred as the AlterWAN data path), but if said destination address of said received IP packet is not an IP address of a computer or other computing device at said destination site, concluding said IP packet is ~~nont~~ an AlterWAN inner ~~payload~~ packet and needs to be routed like ~~as~~ any other IP packet would be routed;

Claim 8 distinguishes over Provino by the following limitations:

where AlterWAN payload packets are packets having as their destination addresses an address of a computing device ~~addressed to devices~~ at said destination site or said source site, and wherein a computing device ~~computer~~ at said destination site is coupled to a computer ~~computing device~~ at said source site via a second firewall circuit and an AlterWAN data path comprisine of a virtual private network tunnel implemented along a high bandwidth, low latency, low hop count data paths through a public wide area network such as the internet terminating at said source site at an untrusted side of said first firewall circuit and terminating at said destination site at an untrusted side of said second firewall circuit, and wherein conventional packets are packets which are not addressed to any computing device ~~devices~~ at said destination site, said first firewall circuit functioning to encapsulate said AlterWAN payload packets in the payload section of AlterWAN packets which have as their destination address the address of said untrusted side of ~~are addressed to~~ said second firewall circuit at said destination end of said virtual private network tunnel

Claim 9 distinguishes over Provino in the following limitations:

2) examining available ISX/ISP internet service providers that can route ~~AlterWAN~~ packets between said source and destination sites and selecting two or more of such ISX/ISP providers as participating ISX/ISP providers including at least a source ISX/ISP provider and a destination ISX/ISP provider through which ~~AlterWAN~~ packet data passing between said source and destination sites will be routed, said selection of said participating ISX/ISP providers being made upon the availability to said participating

ISX/ISP providers of one or more high bandwidth, low latency data paths which will form part of said AlterWAN data path, said participating ISX/ISP providers agreeing to route packets travelling between said source site and said destination site (hereafter AlterWAN packets) into said AlterWAN data path and agreeing to allow route statements to be added to their routers to cause AlterWAN packets to always be routed into said AlterWAN data path, ~~so as to minimize the number of hops on the internet the routers at participating ISX/ISP providers will cause AlterWAN packets to take while traveling between said source and destination sites and so as to~~ said participating ISX/ISP providers also agreeing to manage their portions of said AlterWAN data path so as to guarantee that the average available bandwidth of their portion of said AlterWAN data path ~~the data paths along which said AlterWAN packets traveling between computers at said source and destination sites will travel~~ is substantially greater than the worst case bandwidth consumption of AlterWAN packet traffic between said source and destination sites;

3) adding route statements to routers of said participating ISX/ISP providers which will to cause AlterWAN packets to always be routed into said AlterWAN data path and pretesting said ~~the~~ ISX/ISP providers selected in step 2 by testing to verify the data path that ~~an~~ AlterWAN packets travel will be a portion of said AlterWAN data path and that performance is adequate;

Claim 10 distinguishes over Provino by at least the following limitations:

one or more routers of ~~other~~ participating ISX/ISP providers of internet services including a router at an endpoint participating ISX/ISP provider, said routers of said ISX/ISP providers functioning to implement said AlterWAN data path as a high bandwidth, low latency, low hop count data path having an average available bandwidth that exceeds the worst case bandwidth consumed by incoming and outgoing AlterWAN packets travelling between said source and destination sites,

NEW CLAIMS 11-19

New claims 11-19 have been added to claim various aspects of the invention. All the claims share the same inventive concept: AlterWAN packets are recognized at the ISX routers by their destination IP addresses and routed into a high bandwidth, low latency, low hop count data path.

New claim 11 covers a method of doing business that cover how the source and destination sites are set up, how the ISX/ISPs are selected and how their routers are tested to make sure they contain the proper routing statements to recognize AlterWAN packets and route

then only into high bandwidth, low latency, low hop count data paths and how the source and destination sites are connected to the participating ISX/ISPs through dedicated high bandwidth, low latency data paths.

New claim 12 covers the method carried out at the source end of a private WAN using the internet as the backbone and with the source router recognizing the AlterWAN packets and routing them onto dedicated high bandwidth lines that couple to participating ISX/ISP internet service providers with routers which have been configured to recognize AlterWAN packets and route them into high bandwidth, low latency, low hop count data paths.

New claim 13 covers the receiving end process, and new claim 14 covers a method of doing business in selecting ISX/ISP providers and configuring their routers to implement the invention using composite AlterWAN packets (encrypted) and new claim 15 covers the same as claim 14 but using non encrypted AlterWAN packets.

New claim 16 covers a method of operating a router at an ISX to recognize and route non encrypted AlterWAN packets, and new claim 17 covers the same for encrypted composite AlterWAN packets. New claims 18 and 19 cover routers which have been configured to recognize and route non encrypted and encrypted AlterWAN packets into the high bandwidth, low latency, low hop count data path.

All the new claims include limitations which distinguish them over the prior art in the routing of AlterWAN packets using the destination address as a clue to force them to be routed into the AlterWAN high bandwidth, low latency data path.

Respectfully submitted,

Dated: February 28, 2005

Ronald Craig Fish
Reg. No. 28,843
Tel 408 778 3624
FAX 408 776 0426

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to: Commissioner for Patents , P.O. Box 1450, Alexandria, Va. 22313-1450.
on 2/28/05
(Date of Deposit)

Ronald Craig Fish, President
Ronald Craig Fish, a Law Corporation
Reg. No. 28,843